FUNDAÇÃO UNIVERSIDADE FEDERAL DE RONDÔNIA – UNIR
***CAMPUS* PROFESSOR FRANCISCO GONÇALVES QUILES**
DEPARTAMENTO ACADÊMICO DE CIENCIAS CONTÁBEIS

THIAGO RAFAEL LISOWSKI NASCIMENTO

SEGURANÇA DA INFORMAÇÃO: SUA UTILIZAÇÃO PELOS PROFISSIONAIS DE ESCRITÓRIOS CONTÁBEIS EM PIMENTA BUENO – RO

Trabalho de Conclusão de Curso

Artigo Científico

Cacoal – RO
2014

THIAGO RAFAEL LISOWSKI NASCIMENTO

SEGURANÇA DA INFORMAÇÃO: SUA UTILIZAÇÃO PELOS PROFISSIONAIS DE ESCRITÓRIOS CONTÁBEIS EM PIMENTA BUENO – RO

Artigo – Trabalho Conclusão de Curso apresentado à Fundação Universidade Federal de Rondônia – UNIR – C*ampus* Professor Francisco Gonçalves Quiles como requisito parcial para obtenção do grau de Bacharel em Ciências Contábeis, sob orientação do Prof.º Ms. Rogério Simão.

Cacoal – RO
2014

FUNDAÇÃO UNIVERSIDADE FEDERAL DE RONDÔNIA – UNIR
***CAMPUS* PROFESSOR FRANCISCO GONÇALVES QUILES**
DEPARTAMENTO ACADÊMICO DE CIÊNCIAS CONTÁBEIS

O Artigo - TCC intitulado "Segurança da informação: sua utilização pelos profissionais de escritórios contábeis em Pimenta Bueno – RO", elaborado pelo acadêmico Thiago Rafael Lisowski Nascimento, foi avaliado e julgado aprovado pela banca examinadora formada por:

_____

Prof.º Ms. Rogério Simão
Presidente

_____

Prof.º Ms. Evimael Alves Teixeira
Membro

_____

Prof.ª Dra. Estela Pitwak Rossoni
Membro

_____
Média

Cacoal – RO
2014

Agradeço primeiramente a Jeová Deus, por me prover a vida e saúde durante essa jornada, bem como a companhia de pessoas especiais que me foram de grande ajuda.

À minha família, pelo total incentivo, e pelo amparo nas horas difíceis.

Ao meu orientador, pela colaboração e paciência com que me auxiliou para atingir os objetivos desse trabalho.

Aos professores e colegas que me acompanharam nessa jornada e sempre me ajudaram a vencer os obstáculos ao longo do caminho.

SEGURANÇA DA INFORMAÇÃO: SUA UTILIZAÇÃO PELOS PROFISSIONAIS DE ESCRITÓRIOS CONTÁBEIS EM PIMENTA BUENO, RO

Thiago Rafael Lisowski Nascimento[1]

Resumo: Esta pesquisa teve como objetivo evidenciar ações adotadas pelos escritórios de contabilidade de Pimenta Bueno, RO que proporcionam segurança às informações, tendo em conta o grande volume de informações que os mesmos manuseiam e a necessidade de serem mantidas em segurança. A pesquisa realizada foi bibliográfica de natureza exploratório-descritiva com abordagem qualitativa dos dados, seguida de pesquisa de campo realizada em cinco escritórios de contabilidade. Foram aplicadas quatro entrevistas a gestores e um questionário estruturado a trinta e sete funcionários no período de abril e maio de 2014. Após tabulação e categorização, os dados foram analisados à luz da literatura sobre gestão da segurança da informação. Foram identificadas as ações adotadas que garantem a segurança da informação, segundo três camadas indicadas na literatura: física, lógica e humana. A pesquisa evidenciou que as principais práticas de segurança da informação são: uso do *antivírus*, o monitoramento das instalações por empresa prestadora de serviços de proteção e adoção de políticas de segurança da informação. Conclui-se que, as principais deficiências de segurança encontram-se na camada humana, como, a falta de treinamento relacionado a segurança da informação, tendo em contrapartida a camada física que por tratar de ativos corpóreos e palpáveis facilmente destacam-se quanto a serem assegurados.

Palavras – Chave: Escritórios de contabilidade. Práticas de segurança da informação. Segurança da informação.

1 INTRODUÇÃO

Ao decorrer do processo de desenvolvimento tecnológico, a informação talvez tenha se tornado o ativo mais valioso nas empresas, isso aumenta a responsabilidade dos escritórios de contabilidade em manter a segurança, confiabilidade e disponibilidade das informações. A segurança da informação tem por objetivo garantir a integridade, confiabilidade, confidencialidade, autenticidade, e disponibilidade de informações processadas pela instituição (BRASIL, 2012).

Com a automação dos computadores, os sistemas de informação passaram a concentrar os dados e informações em arquivos de computador que, são acessados por um grande número de pessoas tanto dentro como fora das organizações, desta maneira tais dados são mais propensos à destruição, fraude, erro e uso indevido. Em face das mudanças que vem ocorrendo no ramo da tecnologia da informação nas últimas décadas, destacando-se o início do século XXI, tornando-se cada vez mais necessária a proteção das informações e sua correta utilização em camada física, lógica e humana (LAUDON e LAUDON, 2001).

Segundo Campos (2007), as empresas geralmente fazem seguros de seus bens, sejam eles imóveis, carros e outros bens de valor porque entendem a necessidade de protegê-los contra incidentes que venham a violar sua segurança. Porém, quando se trata de investir na segurança

[1] Acadêmico concluinte do curso de Ciências Contábeis da Fundação Universidade Federal de Rondônia – *Campus* Professor Francisco Gonçalves Quiles, com TCC elaborado sob a orientação do Professor Ms. Rogério Simão.

dos dados e informações da organização, muitos veem como algo adiável ou sem necessidade. Para Batista (2005), visto que as empresas dependem de informações precisas e confiáveis para a tomada de decisões, a busca por mecanismos e ferramentas que auxiliem os profissionais a definirem a melhor maneira de estudar as informações é fundamental para os proprietários e administradores de empresas.

Nesse sentido, esta pesquisa se propôs a responder o seguinte questionamento: que ações adotadas pelos escritórios de contabilidade de Pimenta Bueno – RO proporcionam segurança às informações contábeis? Para isso, buscou-se analisar as ferramentas de segurança da informação adotadas pelos escritórios; identificar de que maneira a segurança da informação é utilizada pelos escritórios contábeis e evidenciar o conceito e a aplicação das normas de segurança da informação.

A pesquisa justifica-se, pois, percebe-se que o universo digital está sujeito às mais variadas formas de ameaças, tanto físicas como virtuais que podem comprometer seriamente o sigilo e integridade das informações. Essas informações, que podem estar na forma de notas fiscais e recibos, documentos cadastrais entre outros, precisam ser asseguradas quanto à sua integridade e sigilo, por motivos éticos e estratégicos. Assim sendo, as empresas estão tomando medidas para combater os ataques a segurança da informação (STAIR e REYNOLDS, 1999).

2 REFERENCIAL TEÓRICO

O referencial a seguir é disposto em tópicos sequenciais onde inicialmente apresenta-se uma evolução história da tecnologia da informação (TI), seguido de uma explanação sobre algumas das principais ameaças aos sistemas de informação. Logo após, apresenta-se o conceito de segurança da informação. Como defesa às ameaças, conceitua-se princípios básicos da política de segurança da informação bem como suas características e benefícios. Por fim, comenta-se sobre as ações de segurança nos sistemas de informação, subdividindo-as em: camada física, lógica e humana.

2.1 EVOLUÇÃO HISTÓRICA DA TECNOLOGIA DA INFORMAÇÃO

No decorrer da história humana, os sistemas foram evoluindo até o início do século XVIII, quando outros tipos de sistemas se destacaram na época, por exemplo: Taylor, com a administração científica e os processos administrativos. Fayol, com o sistema de centralização

e organização formal e impessoal. Weber, com o sistema de burocracia empresarial. Esses modelos de empresa e sistemas deram o direcionamento de como se desenvolveriam as relações entre esses campos.

Para Cruz (2000), durante muito tempo as empresas caracterizavam a tecnologia da informação apenas como um pequeno Centro de Processamento de Dados (CPD), o lugar onde trabalhavam analistas, programadores, e onde ficavam os computadores. O autor continua ainda, por afirmar que eram tempos em que a informática servia mais aos objetivos da própria tecnologia e sua gestão que aos objetivos da empresa, os usuários mantinham distância daquele ambiente, dificultando a interação prática dos sistemas ocasionando assim muito erros. Nesse período inicial de utilização da informática pelas empresas, essa característica elitista era quase justificável diz Cruz (2000), que explica seu posicionamento primeiramente por levar em conta que a tecnologia era caríssima, problemática para manter, difícil de usar e causava muita dor de cabeça aos usuários, dessa forma, era natural que os usuários tivessem um olhar misto de revolta e respeito por parte dos técnicos e suas máquinas, afinal eles eram um pessoal caro e especializado que podia resolver os problemas dos usuários bem como causar mais problemas.

O autor acrescenta que a tecnologia da informação não se chamava assim no início de sua utilização nas empresas, essa tecnologia que começava a se infiltrar nas organizações tinha outros nomes: computadores, sistemas de tratamento da informação, máquina de processamento de dados, sendo que o pior deles talvez tenha sido cérebro eletrônico. Com o passar do tempo, e com a evolução de tais sistemas foi acontecendo uma junção de vários especialidades na utilização do computador, por isso, essa tecnologia já foi chamada de telemática, informática entre outros, até adquirir a que tem hoje: Tecnologia da Informação (TI). A tecnologia da informação tem sua utilização voltada a dar ao usuário o controle efetivo da informação além de simplificar a operacionalidade de sua atividade (CRUZ, 2000).

De acordo com Tanembaun e Wetherall (2011), a tecnologia da informação representada pelas redes de computadores, durante décadas de existência foram utilizadas principalmente por pesquisadores universitários e também por funcionários de empresas para compartilhar impressoras onde, nessas condições a segurança nunca precisou de maiores cuidados. Porém, quando milhões de pessoas comuns passaram a utilizar as redes para executar operações bancárias, fazer compras e realizar transações e registros contábeis, surgiu um ponto fraco atrás de outro, tornando a segurança um problema de grandes proporções tanto às empresas quanto aos usuários domésticos.

Tanembaun e Wetherall (2011), afirma ainda, que a forma mais simples de segurança abrange a preocupação em impedir que pessoas mal-intencionadas leiam ou, pior ainda,

modifiquem secretamente mensagens enviadas a outros destinatários. Por conseguinte, apresenta-se a seguir algumas ameaças comuns aos sistemas de informação.

2.2 AMEAÇAS A SISTEMAS DE INFORMAÇÃO

A segurança da informação é um dos principais focos de atenção na segurança dos nos negócios empresariais, em virtude da preocupação com eventos de insegurança, os escritórios de contabilidade devem estar preparados para enfrentar ocorrências típicas de segurança patrimonial, como o furto de equipamentos e dispositivos móveis e até mesmo interceptação de linhas de comunicação sigilosas, diz Laudon e Laudon (1999). Os autores acrescentam que "as principais ameaças aos sistemas de informação computadorizados são desastres, como incêndios ou falhas elétricas, mau funcionamento do *hardware*, erros de *software*, erros de usuários, e mau uso de computador".

As ameaças à segurança da informação podem ocorrer de natureza física, lógica ou humana. Visto que as informações estão guardadas em locais corpóreos: edifícios, cofres de segurança, ou até dispositivos eletrônicos móveis, esses locais podem estar sujeitos a ameaças tanto naturais (terremotos, inundações, incêndios), como por ação humana (incêndio criminoso, quedas acidentais). Dentre as ameaças lógicas, pode ocorrer o acesso e utilização ilegítima da informação, a interceptação de comunicações e outras ações criminosas, tais como fraude de informática, espionagem, sabotagem, danos em dados e programas. A ligação existente entre os sistemas de informação constitui um fator de risco acrescido para a vulnerabilidade desses sistemas, uma vez que a comunicação pode ser mais facilmente interceptada e os dados desviados (VAZ, 2007).

Conforme Laudon e Laudon (2001), a grande vulnerabilidade dos dados gerou uma preocupação nos construtores e usuários de sistemas de informação, preocupações que incluem desastres, segurança e erro administrativo. Os desastres podem ocorrer em qualquer organização, sendo eles, incêndios, falhas de energia ou outros desastres. Para evitarem perda total de informações, empresas multinacionais tem implantado sistemas de computadores tolerantes a falhas que dispõe de energia, *hardware*, *software* que mantém o funcionamento para prevenir falhas no sistema, essa tecnologia é usada por empresas para aplicações críticas com pesadas exigências de processamento de transações *on-line*. A segurança se refere às políticas, procedimentos e medidas técnicas usadas para prevenir acessos não-autorizados ou alteração, roubo e danos físicos aos sistemas de informação. Em relação aos erros, observa-se

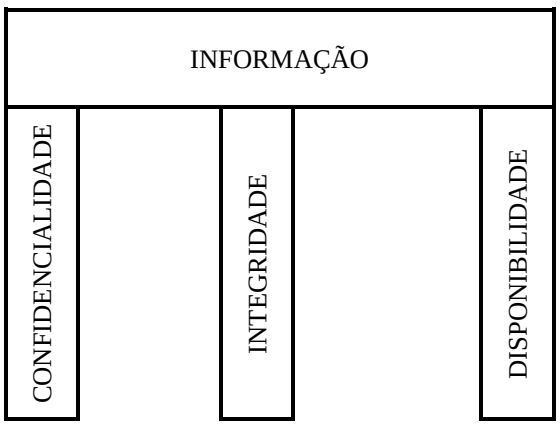
que os próprios computadores podem servir como instrumentos de erro que podem ocorrer em vários pontos de um ciclo de processamento: por meio da entrada de dados, erros de programas, operações de computador e *hardware*. Tendo em vista tais ameaças, conceitua-se a seguir a segurança da informação e suas principais características.

2.3 CONCEITO DE SEGURANÇA DA INFORMAÇÃO

Em sua introdução a ABNT NBR ISO/IEC 17799 (2005), define segurança da informação como "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio". A segurança da informação visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela instituição (BRASIL, 2012). De acordo com Laudon e Laudon (2001), algumas empresas que dependem de computadores para desempenharem suas funções podem perder todo seu espaço no mercado empresarial se mesmo que por alguns instantes perderem sua capacidade computacional.

A concentração de recursos nos computadores torna a violação da segurança da informação um aspecto de grandes perdas e alto risco para as empresas, podendo até mesmo gerar prejuízos que levem a organização a uma situação deficitária irreversível. Tanto para Campos (2007), quanto para Goodrich e Tamassia (2013), um sistema de segurança da informação tem base em três princípios básicos: confidencialidade; integridade e disponibilidade. A figura a seguir, demonstra tal conceito defendido por Campos (2007).

FIGURA 1: Pilares de um sistema de segurança da informação



Fonte: Campos (2007) adaptado pelo autor

Como observado na Figura 1, não sendo aplicado em algum momento qualquer um desses princípios, caracteriza-se quebra de segurança da informação. Analisa-se a seguir, o conceito de cada um dos pilares da segurança da informação.

2.3.1 Confidencialidade

Para Campos (2007), "o princípio da confidencialidade é garantido quando apenas as pessoas explicitamente autorizadas podem ter acesso à informação." Havendo acesso à informação por pessoa não autorizada, tanto pela descoberta de senhas como por acesso a documentos ou de qualquer outro modo, intencionalmente ou não, caracteriza-se quebra de confidencialidade. Pode também ocorrer de maneira muito mais discreta, como quando pessoas que trabalham em uma determinada organização conversam sobre os assuntos de trabalho, muitas vezes confidenciais, em locais públicos, como restaurantes, lanchonetes, elevadores, deixando assim informações importantes irem ao conhecimento daqueles a sua volta. De acordo com Marçula e Filho (2005), os dados armazenados nos computadores não devem ser revelados a pessoas que não tenham autorização para acesso, é preciso manter a privacidade.

Num cenário de ameaças por todo o redor, pesquisadores de segurança de computadores e projetistas de sistemas tem desenvolvido muitas ferramentas para proteger informações sensíveis. Goodrich e Tamassia (2013) evidenciam algumas ferramentas que incorporam esses conceitos, conforme demonstrado no quadro à seguir:

QUADRO 01 – Conceitos de ferramentas de segurança da informação

Ferramentas	Conceito
Controle de acesso	Regras e políticas que limitam o acesso a informação confidencial apenas para aquelas pessoas com uma necessidade de saber. Tal necessidade pode ser determinada por identidade, como o nome da pessoa, pelo papel que ela desempenha, como ser um gerente ou funcionário.
Autenticação	A determinação da identidade ou do papel de alguém. Geralmente é baseada em uma combinação de três fatores: algo que a pessoa tem (como um cartão, ou dispositivo que armazena chaves secretas), algo que a pessoa sabe (como uma senha) e algo que a pessoa é (sua impressão digital, retina dos olhos).
Autorização	A determinação se uma pessoa tem permissão a acessar os recursos, com base em uma política de controle de acesso. Tal recurso deve evitar que o sistema seja enganado e permita acesso a seus recursos protegidos a pessoas não autorizadas.
Segurança Física	São barreiras estabelecidas fisicamente para limitar o acesso a recursos computacionais protegidos, incluem cadeados em portas ou gabinetes, colocação de computadores e servidores em salas sem janelas, uso de materiais sólidos de isolamento.

Fonte: Elaborado pelo autor, baseado em Goodrich e Tamassia (2013)

Conforme observado no quadro 1, a confidencialidade num contexto de segurança de computadores, é evitar que informações sejam reveladas sem autorização, a proteção de dados propiciando acesso àqueles que são autorizados a vê-los e não permitindo que outros saibam algo a respeito de seu conteúdo.

Para exemplificar como esses conceitos são colocados em prática, Goodrich e Tamassia (2013) explicam que quando se visita uma página da *internet* que pede o número de nosso cartão de crédito e o navegador exibe um pequeno ícone de cadeado no canto, o navegador faz um processo de autenticação para verificar se o *site* com o qual se está conectando é de fato quem diz ser. Enquanto isso, o próprio *site* verifica se o navegador que está sendo utilizado é autêntico e se há autorização para acessar essa página da *Web*. O navegador então, solicita ao *site* uma chave de encriptação para codificar o cartão de crédito e quando o número do cartão alcança o servidor que está fornecendo o *site*, o centro de dados do banco onde o servidor está localizado deve ter níveis adequados de segurança física e políticas de acesso para manter os respectivos dados seguros.

2.3.2 Integridade

A integridade é importante pois explica que a informação não deve ser alterada de maneira não autorizada. As ferramentas para proteger a confidencialidade da informação mencionadas no Quadro 1, também ajudam a evitar que dados e informações sejam modificados. Existem várias ferramentas especialmente projetadas para apoiar a integridade, sendo uma delas as cópias de segurança: o arquivamento periódico de dados, sendo efetuado de modo que os arquivos possam ser restaurados caso tenham sido alterados de maneira não autorizada ou não intencional (GOODRICH e TAMASSIA, 2013).

De acordo com Marçula e Filho (2005), integridade diz respeito aos dados armazenados nos computadores serem mantidos íntegros, corretos, não devendo ser perdidos. Além disso, deve haver garantia de que é possível reconhecer e recuperar as falhas de integridade, podendo tais falhas serem acidentais ou intencionais.

2.3.3 Disponibilidade

Para Goodrich e Tamassia (2013), a disponibilidade relaciona-se à informação ser acessível e modificável no momento oportuno por aqueles que estejam autorizados a fazê-lo.

Disponibilidade refere-se aos serviços oferecidos pelos computadores serem mantidos disponíveis aos usuários. Isso deve incluir a garantia que: serviços não sejam interrompidos, mesmo em casos de falhas (de *hardware* ou *software*), ou durante rotinas de manutenção do sistema; que seja possível reconhecer e recuperar a disponibilidade dos serviços quando houver incidentes relacionados à segurança (MARÇULA e FILHO, 2005).

A normativa ABNT NBR ISO/IEC 27001 (2006), define um conjunto de boas práticas para a gestão da segurança da informação que foi elaborada para estabelecer um modelo de implementação, operação, monitoração e revisão para certificação de sistemas de segurança da informação, descreve requisitos para a implementação de controles de segurança customizados para as organizações. Consoante a Marçula e Filho (2005), a normativa dispõe que a segurança da informação tem como premissas básicas a preservação da confidencialidade, integridade e disponibilidade da informação. Outra função da segurança da informação é garantir a autenticidade, responsabilidade e confiabilidade das informações. A seguir são relacionados pontos essenciais de segurança da informação definidos pela normativa:

a) Evento de segurança da informação: é a ocorrência identificada de um sistema, serviço ou rede que demonstre possíveis violações das políticas de segurança da informação ou falha de controles, ou de situações desconhecidas, que possa ter impacto na segurança da informação;

b) Incidente de segurança da informação: é um simples (ou série de) evento(s) indesejado(s) ou inesperado(s), que tenha grande chance de impactar a operação da organização e ameaçar as informações;

c) Sistema de gestão da segurança da informação: baseada em uma aproximação de risco empresarial, que deve estabelecer, implementar, operar, monitorar, revisar, manter, aperfeiçoar a segurança da informação.

Para que tais conceitos possam ser aplicados, necessita-se de bons métodos e procedimentos para manter a segurança da informação. Nesse sentido, a definição da política de segurança da informação é considerada a seguir.

2.4 DEFINIÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

De acordo com Araújo e Ferreira (2008), “a política de segurança define o conjunto de normas, métodos, e procedimentos utilizados para a manutenção da segurança da

informação, devendo ser formalizada de divulgada a todos os usuários que fazem uso dos ativos de informação.”

Para seu desenvolvimento e elaboração, os autores defendem o uso de uma visão metódica, criteriosa e técnica de forma que possam ser sugeridas alterações na configuração de equipamentos, na escolha de tecnologias e definição de responsabilidades. Deve também expressar os objetivos dos proprietários ou acionistas, os quais são responsáveis pelas decisões quanto ao uso das informações.

Destacando as características e benefícios da política de segurança da informação Araújo e Ferreira (2008), afirmam que a efetividade de uma política de segurança da informação está diretamente relacionada com algumas características. Tais como as que são abordadas verticalmente no quadro a seguir:

QUADRO 02 - Características e benefícios da política de segurança da informação

<table>
<tr><th rowspan="2">Características</th><th colspan="3">Benefícios</th></tr>
<tr><th>Curto prazo</th><th>Médio prazo</th><th>Longo prazo</th></tr>
<tr><td>Ser verdadeira: Deve evidenciar o pensamento da empresa e ser coerente com as ações da organização. Ser possível seu cumprimento.</td><td>Formalização e documentação dos procedimentos de segurança adotados pela organização.</td><td>Padronização dos procedimentos de segurança incorporados na rotina da empresa.</td><td rowspan="2">Retorno sobre o investimento realizado, por meio da redução dos problemas e incidentes de segurança da informação.</td></tr>
<tr><td>Ser complementada com a disponibilidade de recursos: Deve haver uma liberação de recursos financeiros e de pessoal para que as diretrizes possam ser implementadas ao longo do tempo.</td><td>Implementação de novos procedimentos e controles.</td><td>Adaptação segura de novos processos do negócio.</td></tr>
<tr><td>Ser válida para todos: deve ser cumprida por todos os usuários da informação da organização, sendo válida desde o presidente até o estagiário recém contratado.</td><td>Prevenção de acessos não autorizados, danos ou interferência no andamento dos negócios, mesmo nos casos de falhas ou desastres.</td><td>Qualificação e quantificação dos sistemas de resposta a incidentes.</td><td rowspan="3">Consolidação da imagem corporativa associada a Segurança da Informação.</td></tr>
<tr><td>Ser simples: deve ser de fácil leitura e compreensão.</td><td rowspan="2">Maior segurança nos processos do negócio.</td><td rowspan="2">Conformidade com padrões de segurança, como a NBR ISSO/IEC27002.</td></tr>
<tr><td>Comprometimento da alta administração da organização: deve ser assinada pelo mais alto executivo, demonstrando assim, seu total apoio à política.</td></tr>
</table>

Fonte: Elaborado pelo autor, baseado em Araújo e Ferreira (2008)

Conforme observado no quadro 2, as características destacadas aplicam-se a todos que fazem parte da organização da empresa, havendo colaboração de todos os envolvidos os benefícios serão progressivos a curto, médio e longo prazo. Alguns aspectos imprescindíveis para se determinar normas e diretrizes de acordo com Araújo e Ferreira (2008), são destacadas a seguir:

a) Estabelecimento do conceito de que as informações são um ativo importante da organização;
b) Envolvimento da alta administração com relação à Segurança da Informação;
c) Responsabilidade formal dos colaboradores da empresa sobre a salvaguarda dos recursos da informação;
d) Estabelecimento de padrões para a manutenção da Segurança da Informação.

De acordo com Turban, *et. al.* (2010), o objetivo das práticas de segurança de informação é defender todos os componentes de um Sistema de Informação, especificamente os dados, os aplicativos de software, o hardware e as redes. A seguir, são destacadas algumas ações que visam a segurança das informações nos sistemas.

2.5 FERRAMENTAS DE SEGURANÇA NOS SISTEMAS DE INFORMAÇÃO

Segundo o manual de boas práticas em segurança da informação do Tribunal de Contas da União, os sistemas precisam de segurança

> [...] porque a informação é um ativo muito importante para qualquer instituição, podendo ser considerada atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob conhecimento de pessoas de má-fé ou de concorrentes podem comprometer significativamente, não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais (BRASIL, 2012).

Percebe-se então, que a informação exerce influência impactante nas organizações como ferramenta decisória, ao ser utilizada de maneira incorreta e com intenções prejudiciais pode causar profundos efeitos negativos para a organização se não trabalhada com a devida segurança.

Para Sêmola (2003), a gestão da segurança da informação pode ser classificada em três níveis: físico, tecnológico e humano. As organizações preocupam-se principalmente com o nível tecnológico (redes, *vírus*, *hackers*, *Internet*) e se esquecem dos outros – físico e humano – tão importantes e relevantes para a segurança do negócio quanto o nível tecnológico.

Os controles de acesso, físico ou lógico, tem por objetivo proteger os equipamentos, aplicativos e arquivos contra perdas, modificação, alteração, exclusão ou divulgação não autorizada, Brasil (2012). Por não serem unicamente bens corpóreos, os sistemas computacionais não podem ser facilmente controlados apenas com dispositivos físicos, como cadeados, alarmes ou guardas de segurança, necessitando assim de controles de acesso para que seja garantida segurança a tais sistemas.

2.5.1 Segurança na camada física

É o ambiente onde está instalado fisicamente o *hardware* – computadores, servidores, antenas de transmissão, *modens*, cabos, bem como toda sua infraestrutura de telecomunicação podendo ser o escritório da empresa, a fábrica ou até a residência do usuário no caso de acesso remoto ou uso de computadores portáteis. De acordo com Turban, *et. al.* (2010), "a segurança física refere-se a proteção de instalações e recursos de informática. Isso inclui proteger a propriedade física como computadores, centros de dados, *software*, manuais e redes." Fornecendo também, vários controles como: blindagem contra campos magnéticos; interrupção de energia de emergência e baterias de *backup*; alarmes de detecção de movimentos que detectam invasão física.

Segundo Laudon e Laudon (2001), para que os erros sejam minimizados, desastres, crimes em computadores e brechas de segurança, precisam ser incorporados no projeto e na implantação dos sistemas de informação políticas e procedimentos especiais. O controle consiste em todos os métodos, políticas e procedimentos organizacionais que garantem a segurança dos bens da organização, a precisão e a confiabilidade dos seus registros contábeis e a adesão operacional aos padrões gerenciais. O controle de um sistema de informação precisa ser uma parte integral no projeto de uma organização, tanto usuários como construtores durante toda a vida do sistema estarão dando detida atenção aos controles de segurança.

Dentre tais controles, Laudon e Laudon (2001), destacam os controles de *hardware*, que asseguram que o *hardware* de computador seja fisicamente seguro, e verificam defeitos no funcionamento do equipamento. O *hardware* de computador deve ser fisicamente seguro, de modo que possa ser acessado somente por indivíduos autorizados, devendo também ser protegido especialmente contra incêndios e extremos de temperatura e de umidade. Controles de segurança de dados, asseguram que arquivos valiosos de dados empresariais não estejam sujeitos a acessos não-autorizados, mudanças ou destruição. Tal proteção em camada física

torna-se a ação mais utilizada em virtude de se tratar de bens corpóreos, em que facilmente pode-se estabelecer valores, prejuízos e perdas consequente de ataques de fraudadores ou mesmo eventuais acidentes.

2.5.2 Segurança na camada lógica

Os avanços nas telecomunicações se tornaram uma grande vulnerabilidade para os sistemas informatizados, pois o acesso autorizado ou não-autorizado pode ocorrer em qualquer ponto de acesso da rede. A *internet* por exemplo, por ser projetada para ser acessada com facilidade em qualquer lugar do planeta, oferece seus problemas especiais. Dentre os principais riscos existentes, destacam-se pessoas que conseguem sem autorização acesso a uma rede de computador para proveito próprio, dano criminoso ou prazer pessoal (conhecidos popularmente como *hackers*), *vírus* de computador, brechas na segurança, *software* e dados defeituosos, que causam grandes perdas na produtividade (LAUDON e LAUDON, 2001).

De acordo com Goodrich e Tamassia (2013), com o advento das redes sem fio introduziu-se muitos desafio novos para se manter as informações seguras. O autor cita alguns desafios, que incluem: espionagem de pacotes de dados, isso porque todos os computadores que compartilham o mesmo ponto de acesso sem fio estão no mesmo segmento de rede; intromissão, acontece quando um usuário não autorizado esteja conectado à *internet* por meio do ponto de acesso sem fio de outra pessoa; legitimação de usuários, não é mais possível autenticar um *host* legítimo simplesmente pela sua presença física na rede local, são necessários métodos adicionais para autenticação e autorização.

Com relação a privacidade Goodrich e Tamassia (2013), acrescenta que as redes sem fio se comunicam por meio de ondas de rádio tornando a espionagem muito mais fácil do que nas redes com fio. Para espionar uma rede com fio, um atacante deve conseguir acessar uma *interface* física de rede na LAN, mas em uma rede sem fio, qualquer um com equipamento apropriado podem capturar e inspecionar o tráfego que está sendo enviado pelo ar.

Com relação as redes sociais, Goodrich e Tamassia (2013) alertam que elas podem causar o surgimento de riscos de diversas direções, como esses *sites* oferecem muitos canais de comunicação entre usuários os riscos desses contatos podem ser sérios, visto que comprometer a conta de um usuário em uma rede social permitiria acesso a informação privada que poderia ser usada para facilitar o roubo de identidade, fraude ou assédio. Outro risco de ataque para *sites* de redes sociais que os autores mencionam, é o fato de serem altamente interativas e

dinâmicas. Um exemplo mencionado é que várias redes sociais permitem que terceiros escrevam aplicações que são executadas dentro do domínio de segurança do site, essas aplicações são potenciais facilitadores de ataques. Além disso, visto que os *sites* de redes sociais suportam vários tipos de comunicação interativa de usuários, tornam-se potenciais propagadores para ataques de roteiros por meio de *sites*, esses ataques podem causar a propagação de *links* para programas maliciosos ou anúncios *spam*, que visam comprometer a segurança do computador.

Diante dos riscos apresentados, Araújo e Ferreira (2008) recomendam que as políticas de segurança possuam, pelo menos os seguintes procedimentos: uso obrigatório de *software* anti*vírus* em todos os equipamentos; atualização periódica da lista de *vírus* e da versão do produto; verificação de todo arquivo recebido em e-mail ou download, pelo *software* de anti*vírus* e treinamento adequado que oriente a utilização de anti*vírus* para os usuários.

2.5.3 Segurança na camada humana

Para Araújo e Ferreira (2008), "A política de Segurança não é um manual técnico nem um manual de procedimentos." Ela deve ser escrita de forma clara, para que todos possam entendê-la, dessa forma os funcionários estarão preparados para se adequarem as mudanças consequentes na cultura da empesa, de acordo com os autores isso pode ser feito por meio de avisos (comunicação interna, e-mail, *internet*) sobre os esclarecimentos dos principais pontos, pertinentes ás responsabilidades; palestras de conscientização; elaboração de materiais informativos como, cartazes e guia rápido de consulta; treinamento direcionado (aspectos de segurança relacionados as áreas contábil, comercial, financeira e etc.).

De acordo com a norma ABNT NBR ISO/IEC 27002 (2007), "deve-se garantir que os usuários estejam cientes das ameaças e das preocupações de segurança da informação e estejam equipados para apoiar a política de segurança da organização durante a execução normal do seu trabalho."

Consoante a norma citada acima Araújo e Ferreira (2008), afirma que todos os funcionários da organização devem receber treinamento apropriado e atualizações regulares sobre as políticas corporativas que devem incluir requisitos de segurança, treinamento sobre o uso correto dos recursos de Tecnologia da Informação como, por exemplo, procedimentos de acesso lógico (redes, sistemas aplicativos, e-mail, *internet*) e físico (crachá, salas e ambientes restritos). Nesse respeito, os autores enfatizam que mesmo existindo diversas tecnologias

destinadas à proteção dos ativos de informação, o elemento humano é, sem dúvida, fundamental para que a Política de Segurança da Informação seja implementada de forma eficaz. Sendo que os funcionários que não praticam a segurança da informação, se tornam os elos fracos na corrente se segurança, colocando em risco todo o investimento empreendido.

Em seu artigo sobre melhores práticas em segurança da informação, Faustini (2013) aborda algumas práticas que são aconselháveis serem implantadas em toda e qualquer empresa, no caso dessa pesquisa aplicaremos essas práticas aos escritórios de contabilidade, sendo elas:

a) Certificar-se de que cada funcionário possua apenas uma conta de usuário na rede e que a mesma não possua privilégios de acesso desnecessários ou incompatíveis com o cargo ou função que desempenha;
b) Remover contas de rede inativas (como contas de ex-funcionários);
c) Certificar-se de que todas as contas de usuário de sua rede utilizam senhas "fortes" (de difícil suposição) e que sejam obrigatoriamente trocadas com regularidade;
d) Fazer cópias de segurança (*backup*) de dados regularmente e testes comprovando que as mesmas possam ser recuperadas totalmente;
e) Manter um bom programa *antivírus* instalado e atualizado em todos os computadores da empresa – em especial nos servidores;
f) Estabelecer regras para a utilização da *Internet* e *e-mail*, pois mensagens de correio eletrônico contendo arquivos infectados por *vírus* e acesso a *sites* que automaticamente executam e instalam programas maliciosos em computadores são as duas maiores causas de perca de dados nas empresas; se a rede utiliza roteador, trocar a senha de fábrica bem como o nome do administrador, fazer o mesmo para senhas e nomes de usuário.

Observa-se então, que a segurança das informações abrange as camadas física, lógica e humana em que cada qual respectivamente deve receber atenção por parte dos gestores das organizações quanto a sua implementação. A seguir, apresenta-se a metodologia adotada nesta pesquisa para obtenção e análise dos dados.

3 METODOLOGIA

Foi realizada pesquisa bibliográfica de natureza exploratório-descritiva que, para Prodanov e Freitas (2013), procura descobrir a frequência, natureza, características de um fato, suas causas e relações com outros fatos. Os dados de tal pesquisa foram resumidos por meio de fichamento. As variáveis abordadas foram: conceito e aplicação das normas de segurança da

informação adotadas pelos escritórios de contabilidade, segurança da informação em camadas: física, lógica e humana.

Em seguida, realizou-se pesquisa de campo em cinco escritórios de contabilidade, onde foram entrevistados quatro gestores com objetivo de identificar o conhecimento relacionado aos conceitos de segurança da informação e como são aplicados no escritório. O registro das respostas foi realizado com uso de gravações em áudio, que posteriormente foram transcritas e organizadas com apoio de planilhas eletrônicas de edição de texto. Aplicou-se também, um questionário estruturado composto por perguntas objetivas (questões fechadas) e por perguntas dissertativas (questões abertas) seguindo o modelo de levantamento (*survey*) aos trinta e sete funcionários dos respectivos escritórios no período de abril e maio de 2014. A amostragem foi selecionada considerando-se os escritórios de contabilidade que atuam há mais tempo na cidade de Pimenta Bueno, RO e a quantidade de técnicos e funcionários que possuem (tais informações encontram-se no ANEXO 1). Neste sentido, a amostra é intencional, por conveniência e acessibilidade (PRODANOV e FREITAS, 2013).

Tendo em vista a situação problemática e os objetivos definidos neste trabalho, foi adotada uma abordagem de caráter qualitativo que, conforme Prodanov e Freitas (2013), tem por objetivo gerar conhecimentos de aplicação prática dirigidos a solução de problemas específicos, envolve verdades e interesses locais.

Após isso, os dados foram resumidos em quadros e tabelas, categorizados considerando-se os fatores de segurança da informação evidenciados no referencial teórico, sendo relacionados em camadas física, lógica e humana; interpretados explorando as respostas obtidas na entrevista em contrapartida às obtidas no questionário, para se estabelecer relações de conhecimento e aplicação das normas de segurança da informação. Por fim, as informações resultantes da pesquisa foram transcritas por meio da redação do texto científico para oferecer esclarecimento ao problema de investigação proposto. Todos os dados oferecidos por este trabalho foram usados exclusivamente para fins de estudos acadêmicos, respeitando os princípios éticos existentes.

4 RESULTADOS

Para essa pesquisa foram avaliados cinco escritórios de contabilidade com 41 respondentes divididos em dois grupos sendo, um grupo formado por quatro gerentes e outro formado por trinta e sete colaboradores. De acordo com os respectivos gestores, tais escritórios

atuam em média há 14 anos no município de Pimenta Bueno – RO e atendem em torno de 660 empresas.

Para realizar as atividades diárias constatou-se que são utilizados entre 8 e 16 computadores por escritório que estão conectados à *internet* via *Asymmetric Digital Subscriber Line* – ADSL (Linha Digital Assimétrica para Assinante). Quatro dos escritórios pesquisados utilizam uma rede *Wi-Fi* para acesso à *internet* pelos computadores, três dessas redes *Wi-Fi* são ocultas aos que não fazem parte do quadro de funcionários.

A respeito de manterem atualizados os equipamentos, computadores e servidores, constatou-se que quatro dos escritórios pesquisados atualizam-se a cada dois anos e/ou quando os equipamentos apresentam alguma falha ou danos. Do total de computadores dos escritórios, 60% foram montados em lojas de informática locais. Observou-se também que quatro escritórios possuem servidores com autenticação de acesso à *internet*, o que impede que usuários não autorizados tenham acesso aos documentos da rede ao se conectarem à *internet*.

O uso de dispositivos móveis, como *PEN-DRIVE*/CD/DVD em todos os escritórios pesquisados é permitido, contudo, 57% dos funcionários consultados informaram que o uso deve atender requisitos, dos quais os que foram citados são: para as atividades diárias da empresa e desde que esteja livre de *vírus*, os demais informaram que o uso é permitido livremente. Constatou-se também, que apenas um dos escritórios pesquisados utilizam *software* para monitoramento das atividades dos funcionários. Os *softwares* como sistema operacional, pacote *office* e anti*vírus* de três dos escritórios foram adquiridos diretamente com a fabricante e são legalizados.

Dos funcionários consultados, 59% afirmaram não terem recebido treinamento com relação ao uso correto dos *softwares* de trabalho, contudo, a contratação foi efetuada levando em consideração competências já presentes nos candidatos, os demais receberam treinamento apenas com relação ao sistema contábil utilizado pelo escritório. Quanto à existência de uma política de segurança da informação na organização, 57% dos funcionários tem conhecimento e colocam em prática tais normas. Com relação ao acesso às redes sociais ou outros *sites* não pertinentes as atividades do escritório, 78% dos funcionários tem conhecimento de que não é permitido tal conduta. Segundo 65% dos funcionários pesquisados, o escritório em que trabalham possui uma hierarquia de acesso à informação.

A seguir, os resultados obtidos são analisados e discutidos à luz da literatura sobre gestão da segurança da informação. Adotou-se uma estrutura de análise similar à apresentada no referencial teórico, por camadas de segurança em que são utilizadas pelos escritórios pesquisados.

5 ANÁLISE E DISCUSSÃO

A análise foi dividida de acordo com as camadas de segurança da informação mencionados na pesquisa até o momento, sendo essas: camada física, lógica e humana. Foi adotado tal método de análise objetivando-se tornar claro e evidente ao leitor como os escritórios pesquisados praticam a segurança da informação.

5.1 CAMADA FÍSICA

Os resultados examinados evidenciam a atenção prestada por parte dos gestores com relação a segurança e integridade física dos equipamentos e do patrimônio da entidade.

Relacionado às questões que tinham por objetivo avaliar as ferramentas que os escritórios de contabilidade utilizam para assegurarem a integridade física do banco de dados e informações, constatou-se que todos os escritórios pesquisados individualmente contam com serviços de monitoramento e segurança humano, contando ainda com videocâmaras que monitoram e armazenam as imagens, cerca elétrica e alarme. Conforme Turban, *et. al.* (2010), "a segurança física refere-se a proteção de instalações e recursos de informática. Isso inclui proteger a propriedade física como computadores, centros de dados, *software*, manuais e redes."

Questionados sobre o local onde os computadores que desempenham a função de servidores e banco de dados do escritório ficam localizados, três gestores informaram que tais máquinas ficam na sala da diretoria e que todos os funcionários tem acesso ao local, um gestor informou que apenas o funcionário técnico em TI tem acesso ao local. Observa-se portanto, a necessidade de se manter tais máquinas em locais protegidos de possíveis ataques e com acesso restrito apenas a pessoas autorizadas. Nesse respeito Goodrich e Tamassia (2013), defendem o uso de barreiras estabelecidas fisicamente para limitar o acesso a recursos computacionais protegidos.

A respeito de manterem atualizados os equipamentos, computadores, servidores, constatou-se que quatro dos escritórios entrevistados atualizam-se a cada dois anos e/ou quando os equipamentos apresentam alguma falha ou danos. Araújo e Ferreira (2008), ao definirem conceito de política de segurança da informação, defendem o uso de uma visão metódica, criteriosa e técnica de forma que possam ser sugeridas alterações na configuração de equipamentos e na escolha de tecnologias. Destacando-se portanto, a necessidade de manter os equipamentos de informática sempre atualizados.

Questionados se os computadores foram adquiridos de uma fabricante, marca reconhecida pelo mercado; se tal fabricante oferece garantia e suporte contra possíveis problemas técnicos, constatou-se que apenas um escritório adquiriu seus computadores de uma fabricante reconhecida, os demais afirmaram que seus equipamentos foram montados em loja de informática local. Após o período de garantia os escritórios individual e independentemente contratam assistência técnica e suporte de empresas locais prestadoras de serviços no ramo de informática.

Em vista disso, a vantagem dos computadores adquiridos de uma fabricante reconhecida consiste em ter um suporte especializado, com componentes de qualidade pois, tais marcas estabelecem relações diretas com as empresas desenvolvedoras dos componentes. Para Laudon e Laudon (2001), a grande vulnerabilidade dos dados gerou uma preocupação nos construtores e usuários de sistemas de informação onde, os próprios computadores podem servir como instrumentos de erro que podem ocorrer em vários pontos de um ciclo de processamento.

Verificou-se que dois escritórios contratam assistência técnica de uma loja de informática local que atende ao público em geral, abrangendo aspectos de falha no *hardware* e *software* (não havendo contrato estabelecido entre as empresas referente a segurança das informações armazenadas no disco rígido). Entretanto, o sistema contábil utilizado por tais escritório tem suporte fornecido diretamente pela empresa desenvolvedora do programa contábil por meio de ordem de serviço, *chat on-line* e acesso remoto. Os demais escritórios consultados individualmente contam com suporte e assistência técnica completa de uma empresa local especializada em informática e tecnologia focada em atender empresas de diversos segmentos, que inclui *hardware*, *software* e o programa de sistema contábil.

A pesquisa evidenciou também que os cinco escritórios consultados permitem o uso de dispositivos móveis nos computadores, como *PEN-DRIVES*, CD, DVD, dispositivos esses que três dos escritórios fornecem ao funcionário para uso exclusivo aos interesses do escritório. Em conformidade, 57% dos funcionários consultados informaram que o uso deve atender requisitos específicos, tais como: o uso de *pen-drive* deve ser exclusivamente para as atividades diárias da empresa e desde que esteja livre de *vírus*.

Os demais funcionários informaram que o uso de *pen-drive* permitido livremente. Esta questão era pertinente tendo em vista o potencial risco de infecção de *vírus* que tais dispositivos estão sujeitos. De acordo com Laudon e Laudon (2001) dentre os principais riscos existentes, destacam-se dano criminoso ou prazer pessoal (conhecidos popularmente como *hackers*), *vírus* de computador, brechas na segurança, *software* e dados defeituosos, que causam grandes perdas na produtividade.

5.2 CAMADA LÓGICA

Como forma de manter maior segurança e estabilidade na conexão de *internet*, todos os escritórios consultados utilizam *internet* via *Asymmetric Digital Subscriber Line* – ADSL (Linha Digital Assimétrica para Assinante). Pois de acordo com Goodrich e Tamassia (2013), a *internet* foi originalmente criada como um mecanismo para comunicação confiável entre duas partes por meio de uma rede com fio.

Outro fator questionado foi o uso de uma rede de acesso à *internet Wi-Fi* e se tal rede é oculta ou todos podem visualizá-la. Foi constatado que três escritórios possuem rede *Wi-Fi* oculta para quem não faz parte do quadro de funcionários, os demais escritórios consultados utilizam uma rede cabeada para acesso à *internet*, o que oferece maior estabilidade do sinal e segurança contra invasões e ataques virtuais. Goodrich e Tamassia (2013), citam que o advento das redes sem fio introduziu muitos desafios novos para se manter as informações seguras. Os autores citam alguns desafios, que incluem: espionagem de pacotes de dados, intromissão e legitimação de usuários.

Quatro dos escritórios consultados possuem em seus servidores a autenticação de acesso, que impossibilita um usuário que não faz parte do quadro de funcionários ter acesso aos documentos, dados e informações ao se conectar à *internet* do escritório. Essa autenticação de acesso é uma ferramenta de segurança da informação de extrema importância, pois nos remete a um dos pilares do conceito de segurança da informação, a confidencialidade, que de acordo com Campos (2007), é garantida quando apenas as pessoas explicitamente autorizadas podem ter acesso à informação.

Questionados com relação ao uso de *softwares* para proteção virtual dos computadores, verificou-se que todos os escritórios utilizam *antivírus* em todas as máquinas dos escritórios. Pode-se afirmar que essa é a ferramenta de segurança da informação mais utilizada, tendo em vista sua função vital para a proteção dos *softwares* de computador. Para Faustini (2013), é necessário manter um bom programa *antivírus* instalado e atualizado em todos os computadores da empresa, em especial nos servidores. Isso porque, sua ausência representaria uma grave falha de segurança, expondo os computadores ao risco de diversos ataques virtuais.

A pesquisa identificou que os *softwares* utilizados por dois dos escritórios consultados são legalizados e possuem total suporte técnico de seus fabricantes e desenvolvedores. Esse é também um fator crítico quanto a segurança da informação pois, de acordo com os gestores entrevistados, *softwares* legalizados parecem apresentar maior segurança na instalação e manutenção, não apresentando erros ou falhas. Por outro lado, observou-se que os escritórios

consultados não utilizam nenhum tipo de *software* para monitoramento das atividades dos computadores. De acordo com Laudon e Laudon (1999), erros de *software* são uma das principais ameaças aos sistemas de informação computadorizados.

5.3 CAMADA HUMANA

Questionou-se aos funcionários quanto a receberem treinamento com relação ao uso correto dos *softwares*, ou se a contratação foi efetuada levando em consideração tais competências. Dentre os quais, 60% afirmaram não terem recebido e nem recebem treinamento, a experiência adquirida ao longo do desempenho das atividades diária são as responsáveis por um bom desempenho em seu trabalho. Esse fator pode ser considerado um risco à segurança da informação. De acordo com Araújo e Ferreira (2008), todos os funcionários da organização devem receber treinamento apropriado e atualizações regulares sobre as políticas corporativas que devem incluir requisitos de segurança, treinamento sobre o uso correto dos recursos de Tecnologia da Informação como, por exemplo, procedimentos de acesso lógico (redes, sistemas aplicativos, *e-mail*, *internet*) e físico (crachá, salas e ambientes restritos).

A existência de uma política de segurança da informação também foi questionada nessa pesquisa, o gestor de um escritório informou que possui um contrato de sigilo para todos os colaboradores em que os mesmos assinam um termo de responsabilidade e o regulamento interno do escritório, onde prevê a guarda das informações, tanto as impressas quanto às digitais. Toda e qualquer informação, desde o que se ouve, o que se fala, o que se escreve, até os documentos que se recebe deve seguir as normas do contrato de sigilo. Por outro lado, gestores de três escritórios informaram que existem algumas regras pré-fixadas com relação a quais e como as informações devem ser transmitidas, existem algumas informações que apenas o técnico em Tecnologia da Informação tem acesso. Nesse respeito observou-se uma deficiência por parte da gestão dos escritórios, Araújo e Ferreira (2008), defende que a Política de Segurança não é um manual técnico nem um manual de procedimentos, devendo ser escrita de forma clara para que todos possam entendê-la, dessa forma os funcionários estarão preparados para se adequarem as mudanças na cultura da empesa.

Analisando os dados, evidenciou-se que dentre os funcionários questionados, a grande maioria tem conhecimento da existência da política de segurança da informação. Uma questão abria oportunidade para que comentassem como e de que forma utilizam tais políticas. Algumas das respostas são destacadas a seguir:

a) “Sim, sempre quando necessito.”

b) “Sim, a política de segurança é utilizada pois temos clientes com informações relevantes, documentos empresariais, pessoais, onde as informações são fornecidas aos usuários somente, com autorização do cliente.”

c) “Sim, de forma sigilosa.”

d) “Se uma pessoa vem ao escritório solicitar alguma informação, só é passada através de autorização da empresa.”

De acordo com a norma ABNT NBR ISO/IEC 27002 (2007), é necessário garantir que os usuários estejam cientes das ameaças e das preocupações de segurança da informação para que possam apoiar a política de segurança da organização durante a execução normal do seu trabalho.

Foi questionado se é permitido o acesso a redes sociais ou outros *sites* não pertinentes as atividades do escritório, dois gestores informaram que não é permitido tal conduta, os demais permitem o acesso desde que não interfira nas atividades de trabalho e que a duração do acesso seja de poucos minutos. No grupo dos funcionários a maioria respondeu que não é permitido o acesso a *sites* que não estejam relacionados ao trabalho desempenhado no escritório. O acesso as redes sociais e *sites* que não sejam relacionados as atividades da empresa pode ser considerado um fator crítico que expõe ao risco de invasões aos dados sigilosos do escritório. Goodrich e Tamassia (2013) afirma que várias redes sociais permitem que terceiros escrevam aplicações que são executadas dentro do domínio de segurança do *site*, essas aplicações são potenciais facilitadores de ataques, os autores alertam ainda que, ao comprometer a conta de um usuário em uma rede social o atacante teria acesso a informação privada que poderia ser usada para facilitar o roubo de identidade, fraude ou assédio.

A transmissão de informações entre funcionários do escritório e entre funcionário / clientes também foi questionada levando em consideração o fator sigilo. Por parte dos gestores, ficou evidente a ciência de tratarem toda e qualquer informação com máximo sigilo possível levando em conta a opinião dos próprios clientes que se desagradam, boas práticas e bons costumes relacionados ao ponto em questão, não sendo permitido que informações dos clientes sejam comentadas em conversas paralelas tanto em ambiente de trabalho como fora do escritório. No grupo dos funcionários a realidade é consoante a dos gestores, dentre as principais respostas destacam-se as que focalizam o uso da ética profissional, da sensatez para não atingir a integridade das empresas, discrição por parte dos funcionários, com seriedade e respeito ao cliente, não passar informações de uma empresa para outra, não comentar nada relacionado ao escritório, clientes fora do ambiente de trabalho.

Para Campos (2007), há quebra de sigilo da informação quando pessoas que trabalham em uma determinada organização conversam sobre os assuntos de trabalho, muitas vezes confidenciais, em locais públicos, como restaurantes, lanchonetes, elevadores, deixando assim informações importantes irem ao conhecimento daqueles a sua volta.

A pesquisa se propôs identificar também a existência de uma hierarquia de acesso às informação no escritório. Nessa questão, dois gestores informaram que a hierarquia é definida pelo acesso das informações no programa contábil onde cada funcionário tem seu usuário e senha respectivamente de acordo com o departamento que trabalha. Nos demais escritórios, os gestores informaram que, não existe hierarquia com relação as informações, todos os funcionários tem acesso a todas as informações contábeis de seus clientes.

Essa prática pode até facilitar as atividades diárias do escritório, porém, na ótica que se propõe esta pesquisa, a falta de hierarquia de acesso a informação viola o princípio básico de segurança da informação, sendo este a confidencialidade. Nesse respeito, Marçula e Filho (2005) menciona que os dados armazenados nos computadores não devem ser revelados a pessoas que não tenham autorização para acesso, é preciso manter a privacidade. Goodrich e Tamassia (2013), acrescentam que manter confidencialidade num contexto de segurança de computadores é evitar que informações sejam reveladas sem autorização. A confidencialidade envolve a proteção de dados, propiciando acesso aqueles que são autorizados a vê-los e não permitindo que outros saibam algo a respeito de seu conteúdo. Os autores destacam portanto, a necessidade das informações serem disponibilizadas por níveis de privilégios e permissões, onde apenas pessoas autorizadas tenham acesso a determinada informação.

Ao analisar tais conceitos e aplicações da segurança da informação, cabe salientar a função indispensável dos pilares da segurança da informação mencionados tanto por Campos (2007), quanto por Goodrich e Tamassia (2013), sendo o primeiro deles a confidencialidade, observou-se a aplicação desse princípio nos escritórios que em seus servidores possuem autenticação de acesso à internet; no uso de antivírus para proteção virtual dos computadores; na utilização de uma política de segurança da informação ou mesmo quando as informações dos clientes são utilizadas transmitidas de maneira sigilosa, bem como o utilizarem uma hierarquia de acesso à informação. A aplicação do princípio da integridade foi observada nos escritórios que adquiriram seus computadores de uma marca / fabricante reconhecida pelo mercado; ao realizarem *backup* dos dados frequentemente, no estabelecimento de controles de acesso à informação; bem como no monitoramento e segurança física dos equipamentos. Observou-se também a aplicação do princípio da disponibilidade, de maneira que os escritórios

pesquisados atualizam-se quanto a seus equipamentos com frequência; contam com suporte técnico especializado; bem como os *softwares* utilizados são legalizados.

A seguir, elaborou-se um quadro com o objetivo de evidenciar a relação existente entre conceito e aplicação por parte dos escritórios pesquisados a respeito das normas de segurança da informação:

QUADRO 03 – Evidências teóricas e práticas de segurança da informação identificadas

Medidas de Segurança	Evidências Teóricas	Evidências Práticas Identificadas
Existência de Política de Segurança da informação	Conjunto de normas, métodos, e procedimentos utilizados para a manutenção da segurança da informação. Araújo e Ferreira (2008);	É firmado um contrato de sigilo com os funcionários. Esclarecimento sobre as normas de segurança verbalmente.
Dar ciência da política de segurança aos funcionários	É necessário garantir que os usuários estejam cientes das ameaças e das preocupações de segurança da informação**.** ABNT NBR ISO/IEC 27002	A maioria dos funcionários relataram ter conhecimento das políticas de segurança da informação e colocam-nas em prática.
Confidencialidade das informações	Apenas pessoas autorizadas podem ter acesso à informação, evitando que informações sejam reveladas sem autorização. Marçula e Filho (2005); Campos (2007); Goodrich e Tamassia (2013)	Existe uma hierarquia de acesso as informações no programa contábil. Autenticação de acesso à rede e *internet*.
Integridade das informações	Informações armazenadas devem ser mantidas íntegras, não podendo ser perdidas e devem se manter corretas. Marçula e Filho (2005); Turban, *et. al.* (2010); Goodrich e Tamassia (2013)	Contratação de serviços de monitoramento e proteção. É realizado *backup* diário das informações.
Disponibilidade das informações	Informações serem mantidas disponíveis aos usuários e que não sejam de difícil acesso aos usuários autorizados. Marçula e Filho (2005); Goodrich e Tamassia (2013)	Dispõem de pessoal capacitado para suporte e manutenção dos equipamentos. Contam com suporte técnico relacionado ao programa contábil.
Atualização dos equipamentos	Uso de uma visão metódica, criteriosa e técnica de forma que possam ser sugeridas alterações na configuração de equipamentos e na escolha de tecnologias. Araújo e Ferreira (2008)	Atualizam-se a cada dois anos e/ou quando os equipamentos apresentam alguma falha ou danos.
Utilização de *software* de proteção	É necessário manter um bom programa antivírus instalado e atualizado em todos os computadores da empresa, em especial nos servidores. Araújo e Ferreira (2008); Faustini (2013)	Todos os escritórios utilizam programa *antivírus*.
Comportamento ao lidar com informações sigilosas	Há quebra de sigilo da informação quando funcionários conversam sobre os assunto de trabalho, muitas vezes confidenciais, em locais públicos, deixando assim informações importantes irem ao conhecimento daqueles a sua volta. Campos (2007)	Gestores e funcionários tratam de informações com o máximo de sigilo, discrição, seriedade e respeito. Não passam informações de uma empresa para outra, não comentam nada relacionado ao escritório e clientes, fora do ambiente de trabalho.

Fonte: Elaborado pelo autor

Observou-se no quadro 3, que os escritórios possuem algum entendimento com relação a segurança da informação, transmitindo aos seus funcionários regras claras com relação ao comportamento de devem adotar em relação as informações que trabalham, o aspecto de segurança mais relevante que percebe-se é o que abrange a segurança física das informações, pois todos os escritórios atentaram-se a preservar seus ativos nesse sentido. Como é de se esperar, a segurança lógica também destaca-se quando relacionada ao uso de antivírus, atualizações se *softwares*, suporte técnico e hierarquia de acesso as informações da organização.

6 CONSIDERAÇÕES FINAIS

No desenvolver deste trabalho, constatou-se que as principais ações adotadas pelos escritórios contábeis para garantir a segurança da informação são: o antivírus instalado em todos os computadores e o monitoramento das instalações por empresa prestadora de serviços de proteção, atendendo a um dos objetivos propostos, o de analisar as ferramentas de segurança da informação adotados pelos escritórios de contabilidade de Pimenta Bueno – RO.

Foi possível identificar uma deficiência em relação à segurança física dos computadores que desempenham a função de servidor, pois a maioria encontra-se em local que o acesso não é restrito configurando um risco de violação à integridade e confidencialidade das informações. Outro fator que pode ser considerado uma fragilidade é o uso de rede de *internet Wi-Fi*, o que aumenta a facilidade de espionagem, intromissão de usuários não autorizados que poderiam sobrecarregar o uso da banda de *internet* dificultando ou mesmo impossibilitando o cumprimento das responsabilidades legais dos escritórios em relação a transmissão de documentos aos órgãos governamentais de fiscalização.

Identificou-se também as camadas em que a segurança da informação é utilizada pelos escritórios, fator este que demonstrou-se relativamente uniforme dentre os abordados no trabalho, contudo, observa-se que a camada humana é a mais carente de atenção por parte dos gestores tendo em contrapartida a camada física que por tratar de ativos corpóreos e palpáveis facilmente destacam-se quanto a serem assegurados. Buscou-se também, evidenciar o conceito e a aplicação das normas de segurança da informação, nessa questão observou-se que a dificuldade na implementação de boas práticas de segurança da informação pelos profissionais contábeis se deve a carência de conhecimento do tema. Contudo, fica evidente que o conhecimento que detém é utilizado proporcionando segurança às informações que contabilizam.

Por fim, identificou-se quais ações de segurança da informação são utilizadas pelos escritórios de contabilidade. Destacando-se as seguintes: possuir, praticar e comunicar regras básicas de segurança da informação; adotar atitudes a fim de manter a confidencialidade, integridade e disponibilidade das informações; utilizar *software* para proteção virtual das informações e usar de discrição ao lidar com informações sigilosas.

Esta pesquisa limitou-se a identificar as ações de segurança da informação adotadas pelos escritórios contábeis pesquisados, sem aprofundar-se na análise dos sistemas e programas de contabilidade utilizados, não destacou-se os fatores positivos e negativos que influenciam à implantação de um sistema de segurança da informação. Porém, a contribuição da pesquisa consiste no fato de que identificou-se os aspectos que atendem às normas de segurança da informação, bem como aspectos que carecem de segurança podendo adequar-se às normas apresentadas nesta pesquisa. Verificar os fatores positivos e negativos que influenciam a adoção da gestão de segurança da informação nos escritórios de contabilidade pode ser objetivo de pesquisas futuras.

REFERÊNCIAS

ABNT NBR ISO/IEC 27001. **Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos.** Rio de Janeiro, 2006.

ABNT NBR ISO/IEC 27002. **Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos.** Rio de Janeiro, 2007.

ARAUJO, Wagner Junqueira de. **A segurança do conhecimento nas práticas da gestão da segurança da informação e da gestão do conhecimento.** Tese (trabalho final de curso) Universidade de Brasília, Departamento de Ciência da Informação e Documentação. Brasília: 2009.

BATISTA, Emerson de Oliveira. **Sistemas de Informação: o uso da tecnologia para o gerenciamento.** São Paulo: Saraiva, 2005.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação/ Tribunal de Contas da União.** 4. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.

CAMPOS, André. **Sistema de Segurança da Informação: Controlando os Riscos.** 2. Ed. Florianópolis: Visual Books, 2007.

CRUZ, Tadeu. **Sistemas de informações gerenciais:** tecnologias da informação e a empresa do século XXI. 2. ed. São Paulo: Atlas, 2000.

FAUSTINI, Rodrigo. **Melhores Práticas em Segurança da Informação.** Disponível em: <http://www.faustiniconsulting.com/artigo01.htm>. Acesso em: 12 fev. 2014.

FAUSTINI, Rodrigo. **Segurança é investimento?**. Disponível em: <http://www.faustiniconsulting.com/artigo10.htm>. Acesso em: 12 fev. 2014.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Tadeu de. **Política de Segurança da Informação – Guia Prático para Elaboração e Implementação.** 2. ed. Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores.** Porto Alegre: Bookman, 2013.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de Informação: com *Internet*.** 4. ed. Rio de Janeiro: LTC,1999.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Gerenciamento de Sistemas de Informação.** 3. ed. Rio de Janeiro: LTC, 2001.

MARÇULA, Marcelo; BENINI FILHO, Pio Armando. **Informática: Conceitos e Aplicações.** 1. ed. São Paulo: Erica, 2005.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho cientifico: métodos e técnicas da pesquisa e do trabalho científico.** 2. ed. Novo Hamburgo: Feevale, 2013.

REZENDE, Denis Alcides; ABREU, Aline França de. **Tecnologia de Informação aplicada a sistemas de informação empresariais:** o papel estratégico e dos sistemas de informação nas empresas. 2. ed. São Paulo: Atlas, 2001.

STAIR, Ralph M.; REYNOLDS, George W. **Princípios de Sistemas de Informação.** 4. ed. Rio de Janeiro: LTC, 1999.

TANEMBAUM, Andrew S.; WETHERALL, David. **Redes de Computadores.** 5. ed. São Paulo: Pearson Prentice Hall, 2011.

TURBAN, Efraim; *et. al.* **Tecnologia da Informação para a Gestão: Transformando os Negócios na Economia Digital.** 6. ed. Porto Alegre: Bookman, 2010.

VAZ, Ana. **Segurança da Informação, Proteção da Privacidade e dos Dados Pessoais**. Nação e Defesa, Portugal, v. 117 – 3º Série, p. 35-63, 2007.

APÊNDICE A – QUESTIONÁRIO

Prezado (a) colaborador (a)

Sou acadêmico do 8° período do Curso de Ciências Contábeis e solicito sua cooperação respondendo as questões a seguir, para possibilitar o desenvolvimento do meu Trabalho de Conclusão de Curso (TCC), cujo tema é "Percepção da segurança da informação pelos profissionais de escritórios de contabilidade em Pimenta Bueno".

Por isso gostaria de contar com a sua colaboração para responder às perguntas com seriedade. Informo que os dados coletados serão tratados com sigilo e a identificação só será necessária para dirimir eventuais dúvidas quanto ao preenchimento deste instrumento de pesquisa.

Nossos sinceros agradecimentos pela sua participação.

Thiago Rafael Lisowski Nascimento – acadêmico e pesquisador

Prof.º Ms. Rogério Simão – professor e orientador

Infraestrutura:

1) A empresa atualiza-se quanto a seus equipamentos? Com que frequência?

2) Os computadores da empresa foram adquiridos de uma fabricante, marca reconhecida pelo mercado (DELL, HP, LENOVO, etc.)?

   ☐ Sim ☐ Não ☐ Não sei informar

3) A empresa a qual foram comprados os computadores oferece garantia e suporte contra possíveis problemas técnicos, (se sim, como são asseguradas as informações sigilosas gravadas no HD)?

4) Se não, o escritório possui funcionário / técnico em TI que ofereça esse suporte?

5) Existe uma rede Wi-Fi? Se existe, todos podem visualiza-la ou é oculta?

   ☐ Sim, todos podem visualiza-la. ☐ Sim, a rede é oculta. ☐ Não existe uma rede Wi-Fi

6) O acesso à internet é fornecido por:

   ☐ Via rádio. ☐ ADSL. ☐ Modem.

7) Tem servidores de arquivos com autenticação de acesso à internet?

☐ Sim ☐ Não ☐ Não sei informar

8) É permitido o uso de dispositivos móveis nos computadores da empresa, como pen-drives/CD/DVD?

☐ Não é permitido. ☐ Sim, é permitido livremente.

☐ É permitido, desde que:_____.

Software:

9) Utiliza software para monitoramento da atividade dos computadores?

☐ Sim ☐ Não ☐ Não sei informar

10) Os softwares (S.O., Aplicativos de Escritórios, Antivírus) utilizados pelo escritório são legalizados? Possuem suporte técnico?

☐ Sim ☐ Não ☐ Não sei informar

Treinamento

11) Você recebeu treinamento com relação ao uso correto dos Softwares, ou a contratação foi feita levando em consideração tais competências?

12) Existe alguma política de segurança da informação na organização?

☐ Sim ☐ Não ☐ Não sei informar

13) Você tem conhecimento das políticas de segurança da informação da organização?

☐ Sim ☐ Não

14) Você ás utiliza? De que forma?

15) É permitido acesso as redes sociais ou outros sites não pertinentes as atividades do seu trabalho?

16) Como é tratado o sigilo da informação entre funcionários; e entre funcionários e clientes?

17) Existe uma hierarquia de acesso a informação no escritório?

APÊNDICE B – ENTREVISTA

Infraestrutura:

1) O escritório atua a quanto tempo em Pimenta Bueno?

2) Quantos computadores o escritório possui?

3) Os computadores foram adquiridos de uma empresa, marca reconhecida pelo mercado (DELL, HP, LENOVO, etc.)?

4) A empresa atualiza-se quanto a seus equipamentos, com que frequência?

5) A empresa a qual comprou oferece garantia e suporte contra possíveis problemas técnicos, (se sim, como são asseguradas as informações sigilosas gravadas no HD)?

6) Existe um contrato que assegura as informações armazenadas no HD?

7) Se não, o escritório possui funcionário / técnico em TI que ofereça esse suporte?

8) Existe uma rede Wi-Fi? Se existe, todos podem visualiza-la ou é oculta?

9) O acesso à internet é fornecido por via rádio, ADSL, modem? Tem servidores de arquivos com autenticação de acesso à internet?

10) É permitido o uso de dispositivos móveis nos computadores da empresa, como pen-drives/CD/DVD?

Software:

11) Os softwares (S.O., Aplicativos de Escritórios, Antivírus) utilizados pelo escritório são legalizados? Possuem suporte técnico?

12) Utiliza software para monitoramento da atividade dos computadores?

Treinamento:

13) Os funcionários recebem treinamento com relação ao uso correto dos Softwares, ou as contratações são feitas levando em consideração tais competências?

14) Existe alguma política de segurança da informação na organização?

15) O funcionário tem conhecimento das políticas de segurança da informação da organização?

16) Ele ás utiliza? De que forma?

17) É permitido ao funcionário acesso as redes sociais ou outros sites não pertinentes as atividades do seu trabalho?

18) Como é tratado o sigilo da informação entre funcionários, e entre funcionários e clientes?

19) Existe uma hierarquia de acesso a informação no escritório?

ANEXO 1 – RELATÓRIO DOS ESCRITÓRIOS DE CONTABILIDADE DE PIMENTA BUENO – RO

Spiderware CONSELHO REGIONAL DE CONTABILIDADE - RONDONIA Pág.: 1

Sistema Cadastral **Escritório Individual**

Data: 25/03/2014
Hora: 12:59:19

Núm. Registro C. Interno	Nome Nome Fantasia Endereço Bairro Cidade	CEP Caixa Postal	Del UF	Situação CNPJ Tipo Sociedade Telefone Fax	Proc. Dest. Pun.	Nível Resp. Emp/Ano Dt/Orig. Dt/Fund. Dt/Afast.	Faixa/Ano Dt/Atual Dt/Alvará Dt/Restab.	Cap. Valor Dt/Plenária Dt/Vencimento Dt/Alt. Contrat.
RO-000021/O	JANIO TEODORO VILELA ESCRITÓRIO CONTALEX R GENERAL OSORIO 143 PIONEIROS PIMENTA BUENO	76970-000	009 RO	ATIVO 541.339.049-15 INDIVIDUAL 3451-3802	1	TECNICOS 10 18/11/1992	0 18/11/1992	
RO-000054/O	RUBENS DEMARCHI AV PRESIDENTE KENNEDY 636 PIONEIROS PIMENTA BUENO	78984-000	009 RO	ATIVO 328.051.449-53 INDIVIDUAL 69-3451-2519	1	CONTADORES 0 22/01/1993 04/09/1995 04/09/1995	0 20/04/2006 20/04/2006	0 20/04/2006 20/04/2006
RO-000055/O	IVO LUIZ FERRI AV CARLOS DONEJE, 96-A APIDIA PIMENTA BUENO	78984-000	009 RO	ATIVO 282.063.989-53 INDIVIDUAL 451-3635	1	TECNICOS 6 18/11/1992 04/11/1991	0 18/11/1992	
RO-000373/O	ESC IND ADOLFO CESAR BAPTISTA DA SILVA VISAO CONTABIL AV PRESIDENTE DUTRA, 427 CENTRO PIMENTA BUENO	78984-000	009 RO	ATIVO INDIVIDUAL 451-2625	1	TECNICOS 11 22/08/1998 01/06/1998	0 22/08/1998	
RO-000384/O	ESC IND LEVI DA SILVA ESCRITORIO CONTABIL PONTUAL R ROLIM DE MOURA, 250 CENTRO PIMENTA BUENO	78984-000	009 RO	ATIVO 271.599.572-53 INDIVIDUAL 3451-3752	1	TECNICOS 12 28/12/1998 10/11/1998	0 28/12/1998 06/08/2007	0
RO-000494/O	FRANCIVALDO BEZERRA DOS SANTOS ESCRITORIO RONDONIA AV CASTELO BRANCO 961 PIONEIROS PIMENTA BUENO	76970-000	009 RO	ATIVO 236.228.572-34 INDIVIDUAL 69-454-2240	1	TECNICOS 4 25/08/2001 25/08/2001	0 25/08/2001 31/03/2002	25/08/2001

RO-000513/O	ESC IND NEURALDI VIEIRA CAMPOS ESCRITÓRIO FÊNIX R CASIMIRO DE ABREU, 148 CENTRO 78984-000 009 PIMENTA BUENO RO	ATIVO 277.372.179-91 INDIVIDUAL 69-451-2775	1	TECNICOS 11 13/04/2002 01/04/2002	0 13/04/2002 31/03/2008		0 13/04/2002
RO-000566/O	CLEITON ROQUE ESCRITORIO CONTABIL UNIÃO 596.249.062-20 AV CASTELO BRANCO, 943 - SALA-A/ESC CONTABIL UNINDIVIDUALÃO CENTRO 78984-000 009 3451-7747 PIMENTA BUENO RO	ATIVO	1	TECNICOS 0 18/06/2004 19/05/2004	0 18/06/2004 09/07/2007		0 18/06/2004
RO-000592/O	JUAREZ GOMES TEIXEIRA ESCRITORIO CENTRAL AV PRESIDENTE DUTRA 918/SALA 01 PIONEIROS 76970-000 009 PIMENTA BUENO RO	ATIVO 297.942.502-87 INDIVIDUAL 69-3541-8499	1	TECNICOS 0 23/03/2005 03/02/2005 23/04/2009	0 01/12/2010 31/03/2006		0 18/04/2005
RO-000640/O	JOSÉ ROBERTO DEMARCHI ESCRITORIO CONTABIL JR AV ROLIM DE MOURA 987 ALVORADA 78984-000 009 PIMENTA BUENO RO	ATIVO 204.465.869-00 INDIVIDUAL 69-8426-0420	1	CONTADORES 0 0 30/01/2007 08/01/2007	30/01/2007 31/03/2008		0 09/02/2007
RO-000666/O	CELSON GONCALVES LOURA GONÇALVES CONTABIL R ROLIM DE MOURA 112 PIONEIROS 76970-000 009 3451-4113 PIMENTA BUENO 151 RO	ATIVO 419.438.132-72 INDIVIDUAL	RO 0 17/04/2008	TECNICOS	17/04/2008	18/04/2008	

Núm. Registro C. Interno	**Nome Nome Fantasia Endereço Bairro Cidade**	**Situação CNPJ Tipo Sociedade CEP Del Caixa Postal Telefone UF Fax**	**Proc. Dest. Pun.**	**Nível Resp. Emp/Ano Dt/Orig. Dt/Fund. Dt/Afast.**	**Faixa/Ano Dt/Atual Dt/Alvará Dt/Restab.**	**Cap. Valor Dt/Plenária Dt/Vencimento Dt/Alt. Contrat.**
RO-000684/O	ESC IND ADEMIR VIEIRA CAMPOS CENTRAL CONTÁBIL AV PRESIDENTE DUTRA 918 PIONEIROS 78984-000 009 PIMENTA BUENO RO	ATIVO 326.204.979-49 INDIVIDUAL 3451-8359	RO	TECNICOS 0 01/10/2008	01/10/2008	26/09/2008

Spiderware Sistema Cadastral **Sociedade Contábil / Empresário**

Pág.: 1
Data: 25/03/2014
Hora: 12:59:54

Núm. Registro Interno	C.	Denominação ou Razão Social Nome Fantasia Endereço Bairro CEP Cidade Caixa Postal	Del UF	Situação CNPJ Tipo Sociedade Telefone Fax	Proc. Dest. Pun.	Nível Resp. Emp/Ano Faixa/Ano Dt/Orig. Dt/Atual Dt/Fund. Dt/Alvará Dt/Afast. Dt/Restab.	Cap. Valor Dt/Plenária Dt/Vencimento Dt/Alt. Contrat.
RO-000257/O		ESCRITORIO CONTÁBIL IDEAL LTDA - ME ESCRITORIO IDEAL R CASSIMIRO DE ABREU 354 DOS PIONEIROS 76970-000 PIMENTA BUENO	009 RO	ATIVO 12.012.194/0001-24 SOCIEDADE EMPRESÁRIA 3451-4706		NAO INFOR. 1 23/06/2010 23/06/2010	27/10/2010
RO-000310/O		PB CONTABILIDADE LTDA E-CONT CONTABILIDADE AV CASTELO BRANCO 1065/SL 11 PIONEIROS 76970-000 PIMENTA BUENO	009 RO	ATIVO 14.763.306/0001-04 SOCIEDADE EMPRESÁRIA 3451-7548		NAO INFOR. 3 20/12/2011 02/02/2012 20/12/2011	
Total Registros :		**2**					
RO-000748/O		MARIANE BUENO BUENO CONTÁBIL AV EMBOABAS 32/QD 03 BNH I 76970-000 PIMENTA BUENO	009 RO	ATIVO 579.047.902-20 INDIVIDUAL 3451-3928		NAO INFOR. 3 08/12/2010 18/02/2011	
RO-000790/O		JOELMA LUCIANA OLKOSKI ESCRITORIO IVAI AV ALMERINDO GRAVA 178 ALVORADA 76970-000 PIMENTA BUENO	009 RO	ATIVO 792.590.902-10 INDIVIDUAL 3451-3514		NAO INFOR. 27/02/2014 27/02/2014	